AFJ 28768

Attorney Docket No. 1270-034

PATENT

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents; Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

September 25, 2003
(Date of Deposit)

Date 9/25/03
By _____

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Kawaguchi, Eiji, et. al.

Serial Number: 09/806,653

Filed: July, 23 2001

Title: INFORMATION CARD AND INFORMATION CARD SYSTEM

Examiner: St. Cyr, Daniel
Group Art Unit: 2876

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF UNDER 37 C.F.R. 1.192

This brief is in furtherance of the Notice of Appeal, which was filed in this case on July 24, 2003 and received by the Office on July 28, 2003.

The fees required under CFR 1.17 for the fling of this brief are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. 1.192(c))

I REAL PARTIES IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF INVENTION

VI ISSUE

VII GROUPING OF CLAIMS

VIII ARGUMENT - REJECTIONS UNDER 35 U.S.C. 103

IX APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I. REAL PARTIES IN INTEREST

The real parties in interest in this appeal are Eiji Kawaguchi of Hinosato, Munakata, Fukuoka 811-3425 (JP); Richard Eason of 595 Forest Ave., Orono, ME 04473 (US); and ASA Systems, Inc., a Japanese Corporation having a place of business at 3-3 Nakabaru-Shin-machi, Tobata-ku, Kitakyushu, Fukuoka 804-0003 (JP).

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III. STATUS OF CLAIMS

The status of the claims in this application is as follows:

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims 1 – 11, 13, and 15 – 20 are in the in the application.

B STATUS OF ALL THE CLAIMS

1. Claims canceled: 12 and 14

2. Claims withdrawn from consideration but not canceled: None

3. Claims pending: 1 – 11, 13, and 15 – 20.

4. Claims allowed: None

5. Claims rejected: 1 – 11, 13, and 15 – 20.

C. CLAIMS ON APPEAL

The claims on appeal are claims 1 – 11, 13, and 15 – 20.

IV. STATUS OF AMENDMENTS

On April 30, 2003, the examiner issued a final rejection in response to the Applicant's amendment filed on February 20, 2003. The action stated that the amendment would be entered but that the rejection of claims 1 – 11, 13, and 15 – 20 would stand. Accordingly, the present Appeal asks for allowance of claims 1 – 11, 13, and 15 – 20.

V. SUMMARY OF INVENTION

A basic embodiment of the present invention is an information card having a visible photograph of a card owner displayed upon the card and a memory that stores information data. (*See page 9, line 8 through page 10 line 19; see also page 15 lines 10 – 12; see also page 16, lines 5 – 8; see also FIG. 1*) The information data – which may contain either image data or acoustic data – contains inherent data that is both embedded and steganographically hidden in the information data. (*See page 8, line 5 through page 9 line 7; see also page 10, line 20 through page 14 line 14; see also FIGS. 6; see also FIG. 1*) The inherent data includes data that authenticates a legitimacy of an information card owner. (*See page 9, lines 15 – 18; see also page 10, lines 4 – 9; see also FIG. 7; see also FIG. 1.*). One of the information data or the inherent data has a reproduction of the card owner's visible, card surface photograph. (*See page 16, lines 5 – 8; see also page 10, lines 4 – 9; see also FIG. 1.*)

Additional embodiments of the present invention further include inherent data that indicates either legitimacy of the information card or information card owner. (*See page 17, line 1 through page 18, line 13; see also FIG. 7; see also FIG. 1.*) This additional embodiment or the basic embodiment may further feature a memory that stores a password for permitting the information data to be read from the memory. (*See page 15, lines 10 – 12; see also FIG. 1.*). Furthermore, the information card may further employ customized keys in order to give a permission to extract the inherent data from the information data. (*See page 8, lines 25 – 28; see also page 9, line 19 through page 10 line 3; see also FIG. 1.*) The memory of the present invention may include an IC chip. (*See page 15, lines 17 – 24.*)

Another embodiment of the present invention is a system with information card with a memory that stores information data. (*See page 9, line 8 through page 10 line 19; see also page 15 lines 10 – 12; see also FIG. 3; see also FIG. 1.*) The information data contains at

least one of image data or acoustic data, and includes steganographically hidden inherent data, which is embedded therein. (*See page 8, line 5 through page 9 line 7; see also page 10, line 20 through page 14 line 14; see also FIGS. 6; see also FIG. 1.*) The inherent data is data that authenticates the legitimacy of the information card owner. (*See page 9, lines 15 – 18; see also FIG. 7*) This basic embodiment also a password stored in the memory in order to allow the information data to be read from the memory. (*See page 15, lines 10 – 12.*). A data processing terminal has input means for submitting a password and a password checking means that compares the submitted password against the password stored in the memory. (*See page 7, line 27 through page 8, line 4*; s*ee also page 17, line 17 through page 18, line 4; see also FIG. 3; see also FIG. 1.*). Upon a positive password match, the information data may be read from memory, which is then produced via output means. (*See page 5, lines 8 – 10; see also FIG. 4; see also FIG. 1.*).

Additional embodiments include input means for submitting a customized key on the data processing terminal. (*See also FIG. 3.*). Similarly, inherent data extracting means extracts the inherent data using the submitted customized key, which is produced via an output means for outputting the extracted information (*See page 5, lines 8 – 10; see also FIG. 3; see also FIG. 1.*). A further feature checks the information card's inherent data against inherent read from a host and inherent data entered from an external source. (*See page 15, line 25 through page 16, line 2; see also FIG. 7; see also FIG. 1.*).

Some embodiments further include means for embedding the inherent data. (*See page 8, line 8 through page 14 line 14; see also FIG. 6.*). Means for embedding includes at least one means for converting one of image data and acoustic data to pure binary code data, and then a means for converting binary code to canonical gray code data. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*). The means for embedding also has a means for decomposing one of the pure binary code data to canonical gray code data into bit planes. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*). A third component of the means for embedding is a means for segmenting the bit planes into regions according to

complexity measure. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*). A fourth component includes a means for replacing complex region forming data with the inherent data. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*). Optionally, the means for embedding might additionally have means for performing a conjugation operation upon the inherent data. (*See page 8, line 8 through page 14 line 14; see also FIGS. 2(A) to 2(F); FIG. 6*).

The embodiment might also feature an integrated circuit chip as memory; or have a photograph on the surface of the information card, and one of the information data or the inherent data is image data representing the photograph. ((*See page 15, lines 17 – 24*; *see also page 10, lines 4 – 9; see also FIG. 4*). Extracted inherent data may also be wholly or partly checked against one of inherent data read from a host and inherent data entered from an external source. (*See page 9, lines 15 – 18*; *see also page 10, lines 4 – 9; see also FIG. 7; see also FIG. 1.*)

Another embodiment of the present invention is a system with an information card system with an information card displaying a visible photograph of a card owner and a memory that stores information data. (*See page 9, line 8 through page 10 line 19; see also page 15 lines 10 – 12; see also page 16, lines 5 – 8; see also FIG. 3; see also FIG. 1.*) The information data has one of image data or acoustic data and has steganographically hidden inherent data embedded therein. (*See page 8, line 5 through page 9 line 7; see also page 10, line 20 through page 14 line 14; see also FIG. 6*) One of the information data or the inherent data has a reproduction of the card owner's visible card photograph. (*See page 15, lines 22 – 24.*). A data processing terminal has input means for submitting a customized key, inherent data extracting means for extracting the inherent data with the use of the submitted

customized key, and output means for outputting the extracted inherent data. (*See page 5, lines 8 –10; page 17, lines 13 – 19; see also FIGS 1 and 3.*).

Additional embodiments of the present invention further include memory that stores a password for permitting the information data to be read therefrom. (*See page 17, line 17 through page 18, line 4*; *see also page 7, line 27 through page 8, line 4; see also FIG. 1.*). This memory may have an integrated circuit chip. (*See page 15, lines 17 – 24.*) The data processing terminal further includes input means for submitting a password, password checking means for checking the submitted password against the password stored in the information card to permit the information data to be read from the memory, and output means for outputting the read information data. . (*See page 5, lines 8 –10*; *see also page 14, line 26 through page 15 line 7; see also page 17, line 17 through page 18, line 4*; *see also page 7, line 27 through page 8, line 4; see also FIGS. 1, 3 and 7.*).

The basic embodiment might also include extracted inherent data that is wholly or partly checked against one of inherent data read from a host and inherent data entered from an external source. (*See page 17, line 1 through page 18, line 13; see also FIGS. 1 and 7.*) The basic embodiment might further include means for embedding the inherent data. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*). Means for embedding includes at least one means for converting one of image data and acoustic data to pure binary code data, and then a means for converting binary code to canonical gray code data. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*). The means for embedding also has a means for decomposing one of the pure binary code data to canonical gray code data into bit planes. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*) A third component of the means for embedding is a means for segmenting the bit planes into regions according to complexity measure. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*) A fourth component includes a means for replacing complex region forming data with the inherent data. (*See page 8, line 8 through page 14 line 14; see also FIG. 6*)

VI. ISSUE

1. Whether claims 1 – 11, 13, and 15 – 20 are obvious in light of the cited Rhoads United States Patent 5,636,292, titled "Steganography Methods Employing Embedded Calibration Data", in view of Lofberg's United States Patent 4,582,985, titled "Data Carrier".

VII GROUPING OF CLAIMS

The claims on appeal may be separated into the following three separate groups:

Group I consists of claims 1 – 4 and 13.

Group II consists of claims 5 and 15 – 20.

Group III consists of claims 6 - 11

The claims of each group are intended to stand or fall together.

VIII. ARGUMENT - REJECTIONS UNDER 35 U.S.C. 103

Summary of the Rejections

Claims 1 – 11, 13, and 15 – 20 were rejected as obvious in light of the Rhoads U.S. patent 5,636,292, titled "Steganography Methods Employing Embedded Calibration Data" ("Rhoads", '292) in combination with Lofberg's U.S. patent 4,582,985, titled "Data Carrier" ("Lofberg", '985). In making this rejection, the Examiner asserted that

> "Rhoads discloses a steganography method employing embedded calibration data comprising an information card that stores information data including image data (see figure 24, col. 57, line 30+), wherein the information data includes inherent data that is embedded to the information according to steganography (see col. 2, line 11+); the image is printed on the card (see col. 58, line 58), wherein the image is read using a CCD scanner, and a PIN is used to legitimate the user of the card (see col. 60, line 10+)." *Office Action dated April 30, 2003, Page 2.*

The Examiner likewise asserted that Rhoads discloses that a plurality of code keys are contained in the card and suggests that diskette could be used for the storage medium, but fails to explicitly disclose a memory for storing user information. However, the Examiner asserted that Lofberg discloses a data carrier comprising a memory for storing user identification and, in view of Lofberg's teachings, that "it would have been obvious for a person of ordinary skill in the art at the time the invention was made to employ the well known smart card into the system of Rhoads in lieu of the basic storage medium for storing user's information", as "(s)uch a modification would provide additional storage space to store more information to effectively identify each user". In addition, it was asserted that the memory of Lofberg "could be used as an alternate means for storing information to identify the users and would provide greater processing capability to enable local processing of users'

transactions, which would (make) the system more effective and more practical". *Office Action dated April 30, 2003, Page 3.*

Points of error in rejections

The Applicants respectfully disagree with the assertions made by the Examiner and, as explained in detail below, assert that the Examiner failed to establish a prima facie case of obviousness *(See MPEP §2142)* for three separate reasons.

(1) There would be no motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine and/or modify the reference teachings to obtain an information card having a memory into which inherent data is steganographically embedded, as claimed in each of the claims of Groups I, II and III.

(2) The cited references, whether alone or in combination, fail to teach or suggest an information card having a visible photograph on the card surface and a memory that stores a reproduction of the visible photograph of the card owner displayed upon the card, as claimed in each of the claims of Groups I and III. Further, there would be no motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine and/or modify the reference teachings to obtain an information card having a memory into which is stored a reproduction of the visible photograph of the card owner displayed upon the card.

(3) The cited references, whether alone or in combination, fail to teach or suggest an information card system having a data processing terminal comprising an output means for outputting data stored in memory, as claimed in each of the claims of Groups II and III. Further, there would be no motivation, either in the references themselves or in

the knowledge generally available to one of ordinary skill in the art, to combine and/or modify the reference teachings to obtain an information card system having a data processing terminal comprising an output means for outputting data stored in memory.

(1) Non-obviousness of Groups I – III based upon the limitation that the information card have a memory into which inherent data is steganographically embedded

As noted in the Applicants' Amendment dated February 13, 2003, the PLASTIC CREDIT AND DEBIT CARD SYSTEM disclosed by Rhoads (See col. 57, line 30+) has the following features:

a. An image is printed on the card surface with some optional position fiducials for simplifying the scanning tolerances of the image scanner (Fig. 24).

b. Some personal identification data such as bar code is marked on the card surface (Fig. 24).

c. The visible image data is steganographically embedded with an "orthogonal pattern" or "master snowy image", essentially "noise", which does not contain any data to verify the card user, but rather contains a plurality of "transaction tokens" unique to the particular card (Fig. 24 and col. 59, line 22+).

d. The central network chooses a specific location where it expects to find a "transaction token", consisting of a specific pattern found in the original image, and verifies that the chosen "token" is identical to that stored in the network. In this manner, the network is said to need only a small fraction of the total information embedded in the image to verify the validity of the card (col. 58, line 29+)

e. The PIN is not stored on the card, nor it is used at the point of sale terminal. It is only appended to information sent to the central accounting network as the only method of verifying the card user. (col. 60, line 24+).

No memory devices are equipped with the card disclosed by Rhodes. In fact, the statement that "(t)here are no magnetic strips involved," (col. 58, line 19) clearly teaches that the lack of a memory device is desirable, as a magnetic strip is a recognized type of memory device. Accordingly, there is no embedding of any information into memory, and certainly no steganographic embedding of inherent data, as claimed by the Applicants in the claims of each of Groups I – III.

Notwithstanding Rhodes' lack of a memory device on its card, the Examiner asserted that "Rhodes discloses that a plurality of code keys are contained in the card and suggests that a diskette could be used for the storage medium" and that Rhodes "also discloses a plurality of steganographic uses including a serial number identifying ownership to users who wish to legitimately use and pay for empirical information (see col. 54, line 53+)". The Examiner then uses this as the basis for his combination of Rhodes and Lofberg.

This reasoning is flawed for a number of reasons. First, Rhoads' sole teachings regarding a diskette are that "the encoded signal can be distributed in well known ways, including converted to printed image form, stored on magnetic media (floppy diskette, analog or DAT tape, etc.), CD-ROM, etc" (col. 18, line 66+) and "data encoded according to these principles can be stored in various media, including electronic storage media, disks, diskettes" (col.47, line 36+). Thus, Rhoads teaches that such media devices are available for *off-line* distribution of the "information embedded data" and not to serve as a memory device, either on the card or in connection with its use.

Second, the disclosure found within Rhodes at col. 54, lines 53+, which was cited by the examiner as showing "serial number identifying ownership", has nothing whatsoever to do with the PLASTIC CREDIT AND DEBIT CARD SYSTEM disclosed by Rhoads at col. 57, line 30+, or to the Applicants' claimed information card. Rather, the cited passage is directed to the use of Rhoads' methods to steganographically "watermark" empirical data or "creative property", in a manner similar to those currently used to digitally watermark photographs and other media to allow piracy to be discovered. Steganographic embedding in this context serves the same basic purpose as that described in connection with Rhoads' credit card embodiments; i.e. to provide identification of the media in which the information is embedded and not the legitimacy of the owner of one particular copy. In the passage cited by the examiner, the embedding is performed for the purpose of identifying the ownership of the data or "creative property" so that potential users of the data or "creative property" would be able to identify the owner and purchase the right to legitimately use the property. This use has no bearing on authenticating that the holder of a particular copy as, in this context, it is intended that many, many, copies be made and so embedded. Therefore, the Examiner's reliance upon the above cited passages of Rhoads as suggesting the invention could be used to authenticate an owner of **an information card** is clearly misplaced.

Lofberg likewise fails to provide any such suggestion. Lofberg discloses a data carrier comprising a memory means, designated as reference number "6" in Fig.1, which stores "previously and correspondingly obtained reference bit sequence of finger print data of the card holder" (col.3, line 57+), and some control information necessary to allow a microprocessor to process finger print data (col.5, line 10+). According to Lofberg:

"At the time when a data carrier according to the invention is issued, the

> fingertip pattern of one thumb or of a different finger of the owner is recorded. From the recorded information a reference bit sequence, which is unique for the owner or holder, is calculated and this sequence is stored in memory 6 (FIG. 1). When the holder later on is to identify himself against his data carrier, the fingertip information should again be recorded in order to allow for a comparison against the reference bit sequence. This means substantially two problems. First, it must be safeguarded that the direction of the fingertip relative to the sensing surface will be the same as during the recording of the reference bit sequence or otherwise it must be possible to modify the recorded information with respect to a different orientation of the fingertip. Second, the information which is recorded in the sensing device must be read and processed in a way which is reproducible." *Lofberg, Col. 8, Lines 48 – 55.*

Lofberg goes into great detail in its discussion of the specifics of reading and comparing fingerprint patterns, and places emphasis on the fact that the direct comparison of fingerprints at the identification point eliminates any need for a PIN or verification by a central network. However, because of the supposed "fail safe" identification provided by fingerprint comparison, Lofberg makes no effort to hide the information stored in the memory, and certainly does not embed any information within the memory using steganography, as claimed by the Applicants in the claims of each of Groups I – III.

Finally, the Applicants assert that there would be no motivation to combine the teachings of Rhoades and Lofberg because Rhoades expressly teaches away from the use of the same fingerprint identification techniques taught by Lofberg. In particular, Rhoades states:

> "Applicant is aware of a similar idea employed in the very high precision recording of credit card magnetic strips, as reported in the Feb. 8, 1994, Wall Street Journal, page B1, wherein very fine magnetic fluxuations tend to be unique from one card to the next, so that credit card authentication can be achieved through pre-recording these fluxuations later to be compared to the recordings of the purportedly same credit card.
>
> Both of the foregoing techniques appear to rest on the same identification principles on which the mature science of fingerprint analysis rests: the innate uniqueness of some localized physical property. These methods then

> rely upon a single judgement and/or measurement of "similarity" or "correlation" between a suspect and a pre-recording master. Though fingerprint analysis has brought this to a high art, these methods are nevertheless open to a claim that preparations of the samples, and the "filtering" and "scanner specifications" of Melen's patent, unavoidably tend to bias the resulting judgement of similarity, and would create a need for more esoteric "expert testimony" to explain the confidence of a found match or mis-match. An object of the present invention is to avoid this reliance on expert testimony and to place the confidence in a match into simple "coin flip" vernacular, i.e., what are the odds you can call the correct coin flip 16 times in a row." *Rhoads, Col. 2, line 47 – Col. 3, line 4.*

Because Rhoads specifically seeks to avoid the "esoteric "expert testimony"" required by fingerprint identification systems, and as Lofberg was cited by Rhoads during the prosecution of its patent, it can reasonably be presumed that the above passage was specifically directed to the system of the Lofberg patent. Accordingly, as Rhoads expressly teaches away from fingerprint verification systems, and as Rhoads cited Lofberg as one such system, the Applicants further assert that there would be no motivation to combine the Rhoads and Lofberg references to obtain the Applicants' claimed invention.

For the reasons set forth above, the Applicants assert that the claims of Groups I, II and III are unobvious in light of the cited references and respectfully request that the Board not sustain the Examiner's rejection of the claims of Groups I - III under 35 USC§ 103.

(1) Non-obviousness of Groups I and III based upon the limitation that the information card have a memory into which a reproduction of the visible photograph of the card owner displayed upon the card is stored

The Applicant's further assert that neither Rhoads nor Lofberg teaches or suggests the storage of a reproduction of the visible photograph of the card owner displayed upon the card into a card memory.

In addition to the express teaching of Rhoads away from Lofberg, as asserted by the

Applicants in the Amendment of September 16, 2002, the methods disclosed in the Rhoads reference are primarily directed to Boolean authentication of a signal, computer file, image, card, or the like, rather than the authentication that the holder of such a signal, computer file, image or card is the rightful owner. Accordingly, there is no motivation provided within Rhoads to modify the card to include a memory, or "a reproduction of the visible photograph of the card owner" in order to authenticate that the holder of such a signal, computer file, image or card is the rightful owner.

The Applicants' assertions were supported by the Declarations Under 37 CFR §1.132 of Dr. Mongi Abidi, Dr. Hideki Noda, and Dr. Kyoki Imamura, each of whom declared the "methods disclosed in the Rhoads reference are primarily directed to the authentication of the identity of a signal, computer file, image, card, or the like", and "based upon the teachings of Rhoads, I would have no motivation to modify the Rhoads methods to authenticate that the holder of such a signal, computer file, image or card is the rightful owner." However, the Examiner failed to even acknowledge the fact that these Declarations were filed, let alone consider and rebut them, as required under MPEP §716 et. seq.

The Examiner credits Rhoads with disclosing an information card with "the image . . . printed on the card", as the Applicants do in the claims of Groups I and III. Indeed Rhoads does disclose such an image. However, the examiner is only right by half. The examiner ignores the claim limitation that the information data contained within the memory "comprises a reproduction of the visible photograph of the card owner displayed upon the card." Thus, the embodiments of the Applicants' information card claimed in Groups I and III include two photographs: the first on the surface; and the second – a duplicate of the first – stored within the memory. Applicants' claim fraud-prevention

means, i.e. a second photograph capable of authenticating an identical, visible first photograph, is not disclosed or contemplated by Rhoads.

Lofberg likewise fails to disclose the storage into memory of a second photograph capable of authenticating an identical visible first photograph. Rather, Lofberg uses a memory in a data carrier to store fingerprint and fingerprint scanning data. *See '985, column 10, lines 38 – 42.* No mention is made of the storage of any photograph into memory, or the manual comparison of anything shown on the face of the card with a corresponding thing stored into memory.

However, even if it were erroneously assumed that the storage of fingerprints of Lofberg were the functional equivalent to the storage of a photograph, Lofberg still fails to provide any motivation to combine this with the teachings of Rhoads and, in fact, teaches away from such a modification.

As noted above, Rhoads is directed solely to the authentication of the card and not to the authentication of the user. Conversely, Lofberg represents a completely different approach, in which no effort is made to insure that the card itself is authentic. Rather, Lofberg solely attempted to determine whether the fingerprint data stored in the memory of the card matches the fingerprint data obtained by a live scan of a person seeking to use the card. If this data is a match, the verification device indicates this fact and the transaction is presumably allowed to continue. It is important to note that there is no discretion on the part of the security person, clerk, or any other person who is requesting authentication, in making this determination. Accordingly, no information data is stored in memory to allow such a person to make a contrary determination.

The reason Lofberg avoids in-person data analysis and legitimacy determinations is

readily apparent upon examination of the "Background of the Invention". Lofberg states that:

> "A general problem when data cards are used is the fact that a lost or stolen data card may be used without authorization by a different person. This problem may be eliminated if the user is obliged to verify his right before the data card may be used.
>
> In the case of data cards intended for manual handling, the verification may be carried out in that the user verifies his identity by presenting a different identification document. Normally, however, a certification is not required when such a data card is used, among other things due to the fact that this will create a delay and give rise to a long line of people at the places of use. Instead the active control or check is carried out by means of so-called black lists comprising the numbers of all blocked accounts, which may have been blocked due to the fact the account holder has not fulfilled his obligations towards the accounting organization or the fact that the account holder has reported the card as lost. The black lists, being up-dated regularly, mean a significant increase of work at the places of use. Moreover, it is possible that a blocked account will not be observed during a manual check. As a consequence, the card will be used despite the fact that it should not. Furthermore a card, which has been lost for example, may be misused from the time it is reported as lost until an updated black list is available." *Lofberg; Col. 1, line 46 – Col. 2, line 3.*

As these paragraphs clearly illustrate, the unauthorized use of a lost or stolen card is the problem to be solved, and it is conceded that it is impractical to conduct an in-person verification using an "identification document"; presumably a drivers license, passport, etc., due to the fact that such verification causes delays and gives rise to "a long line of people at the places of use." Given this focus on avoiding the delays caused by in-person verification, the Applicants assert that Lofberg teaches away from the inclusion of any information that could be used during an in-person analysis to make a determination of authenticity. Thus, Lofberg likewise teaches away from the storage of the claimed reproduction of the owner's photograph, as the only purpose of such a photograph would be to enable the same in-person analysis that it seeks to avoid.

Similarly, Rhoads likewise discourages discretion on the part of personnel. Not only does Rhoads not teach this, but his patent description would not tolerate local viewing of steganographically hidden data: "[a]s will be seen, none of the point-of-sale locations ever has knowledge of this image, they merely answer queries from a central network." *See '292, column. 59, lines 20 – 48.*

For the reasons set forth above, the Applicants assert that neither Rhoads nor Lofberg discloses an information card having a visible photograph on the card surface and a memory that stores a reproduction of the visible photograph of the card owner displayed upon the card, as claimed in each of the claims of Groups I and III, and that there would be not motivation to combine and modify the cited references to achieve this result. Accordingly, the Applicants request that the Board not sustain the Examiner's rejection of the claims of Groups I and III under 35 USC§ 103.

(3) Non-obviousness of Groups II and III based upon the limitation that system include a data processing terminal comprising an output means for outputting data stored in memory

Finally, the Applicants assert none of the references disclose a data processing terminal that includes an "output means" for outputting the data stored in memory as claimed in each of the claims of Groups II and III.

As noted above, Rhoads fails to disclose or suggest any memory and, consequently, does not disclose a terminal that includes an output means for outputting data stored therein. Further, the system contemplated by Rhoads performs all processing at the central network and not at a data processing terminal. This is said to be preferred as the information read from the card is not transmitted, but rather a twenty-four dot product, based upon the random numbers generated by

the network and the information upon the card, is transmitted to the network, which authenticates the card and sends only an approval to the data processing terminal. (See Rhoads, FIG. 25 and between column 60, line 39, to column 61, line 31). Given the authentication method disclosed, the card system of Rhoads clearly fails to suggest the inclusion of any "output means" for outputting stored data, let alone for outputting data stored in a non-existent memory. Further, because the system is specifically designed to avoid a transmission of the actual data, there would be no motivation to modify the system of Rhoads to include such an "output means".

These assertions were likewise supported by the above referenced Declarations, with each Declarant declaring that "the card disclosed in the Rhoads reference does not provide any authentication that the user of the card is the owner of the card and does not include any "output means for outputting the read information data", as claimed in the Applicant's claims 5 - 12." Each further declared, "that, because the system disclosed in the Rhoads is specifically designed to avoid a transmission of the actual data, I would have no motivation to modify the system to include such an "output means"." As noted above, the Examiner failed to even acknowledge these Declarations let alone consider and rebut them, as required under MPEP §716 et. seq.

Lofberg likewise fails to disclose or suggest such an output. As explained in detail above, Lofberg provides an output signal that indicates the favorable or unfavorable result of the fingerprint authentication process, but does not output any of the data stored in the memory; i.e the reference signals corresponding to the fingerprints stored in the memory. Such an output signal is likewise not found in any of the other cited references.

With regard to any asserted motivation provided by the references to modify Lofberg to include such an output means, the Applicants point to the remarks set forth above with regard to its teaching away from in-person authentication in rebuttal of such an assertion.

Further, the Applicants note that Lofberg itself teaches away from such an output of stored data as such an output would merely result in the display of a reference bit sequence that corresponds to the authorized user's fingerprint and not to a picture of the fingerprint itself. Accordingly, outputting such data would be of absolutely no benefit in authenticating that the holder of the card it its owner.

For the reasons set forth above, the Applicants assert none of the references disclose a data processing terminal that includes an "output means" for outputting the data stored in memory as claimed in each of the claims of Groups II and III, and that there would be not motivation to combine and modify the cited references to achieve this result. Accordingly, the Applicants request that the Board not sustain the Examiner's rejection of the claims of Groups II and III under 35 USC§ 103.

Conclusion

For the reasons set forth above, the Applicants assert that the claims of Groups I, II and III are unobvious and respectfully request that the Board not sustain the Examiner's rejection of any of the claims.

IX APPENDIX OF CLAIMS

1. An information card comprising a visible photograph of a card owner displayed upon the card and a memory that stores information data, the information data comprising one of image data and acoustic data;

wherein the information data contains inherent data that is embedded in the information data according to steganographic information hiding;

wherein the inherent data comprises data that authenticates a legitimacy of a card owner of the information card; and

wherein one of the information data and the inherent data comprises a reproduction of the visible photograph of the card owner displayed upon the card.

2. The information card according to claim 1, wherein the inherent data further comprises data that authenticates a legitimacy of the information card.

3. The information card according to claim 1 wherein the memory stores a password for permitting the information data to be read from memory.

4. The information card according to claim, wherein the memory employs a customized key in order to give a permission to extract the inherent data from the information data.

5. An information card system comprising:

an information card comprising a memory that stores information data, the information data comprising one of image data and acoustic data, wherein the information data comprises inherent data that is embedded in the information data according to

steganographic hiding, wherein the inherent data comprises data that authenticates a legitimacy of a card owner of the information card, and wherein the memory stores a password for permitting the information data to be read from the memory; and

a data processing terminal comprising input means for submitting a password, password checking means for checking the submitted password against the password stored in the information card to permit the information data to be read from the memory, and output means for outputting the read information data.

6. An information card system comprising:

an information card comprising a visible photograph of a card owner displayed upon the card and a memory that stores information data, wherein the information data comprises one of image data and acoustic data, wherein the information data comprises inherent data that is embedded in the information data according to steganographic information hiding, wherein one of the information data and the inherent data comprises a reproduction of the visible photograph of the card owner displayed upon the card; and

a data processing terminal comprising input means for submitting a customized key, inherent data extracting means for extracting the inherent data with the use of the submitted customized key, and output means for outputting the extracted inherent data.

7. The information card system according to claim 6, wherein the memory stores a password for permitting the information data to be read from the memory, and wherein the data processing terminal comprises input means for submitting a password, password checking means for checking the submitted password against the password stored in the information card to permit the information data to be read from the memory, and output means for outputting the read information data.

8. The information card system according to claim 7, wherein the extracted inherent data is at least partly checked against one of the inherent data read from a host and inherent data entered from an external source.

9. The information card system according to claim 6, wherein said system further comprises a means for embedding the inherent data, said means for embedding comprising:

at least one of a means for converting one of image data and acoustic data to pure binary code data, and a means for converting the pure binary code data to canonical gray code data;

means for decomposing one of the pure binary code data and the canonical gray code data into bit planes;

means for segmenting the bit planes into regions according to a complexity measure, and

means for replacing complex region-forming data with the inherent data.

10. The information card system according to claim 9, wherein the means for embedding the inherent data further comprises means for performing a conjugation operation upon the inherent data.

11. The information card system according to claim 6, wherein the memory comprises an integrated circuit chip.

12. Cancelled

13. The information card according to claim 1, wherein the memory comprises an IC chip.

14. Cancelled

15. The information card system according to claim 5, wherein said data terminal further comprises input means for submitting a customized key, and inherent data extracting means for extracting the inherent data with the use of the submitted customized key, and an output means for outputting the extracted information data.

16. The information card system according to claim 15, wherein the extracted inherent data is at least partly checked against one of inherent data read from a host and inherent data entered from an external source.

17. The information card system according to claim 5, wherein said system further comprises a means for embedding the inherent data, said means for embedding comprising:

at least one of a means for converting one of image data and acoustic data to binary code data, and a means for converting the pure binary code data to canonical gray code data;

means for decomposing one of the pure binary code data and the canonical gray code data into bit planes;

means for segmenting the bit planes into regions according to a complexity measure, and

means for replacing complex region-forming data with the inherent data.

18. The information card system according to claim 17, wherein the means for embedding the inherent data further comprises means for performing a conjugation operation upon the inherent data.

19. The information card system according to claim 5, where the memory comprises an integrated circuit chip.

20. The information card system according to claim 5, wherein the information card carries a photograph on a surface thereof, and one of the information data and the inherent data is image data representing the photograph.

Respectfully submitted,

September 25, 2009
Date

Michael J. Persson
Attorney for Applicant
Reg. No. 41,248

Lawson & Persson, P.C.
67 Water Street, Suite 103
Laconia, New Hampshire 03246
Phone: 603-528-0023
Fax: 603-528-3332